STUDIA UNIVERSITATIS BABEŞ-BOLYAI
Engineering 69(1) 2024 DOI: 10.24193/subbeng.2024.1.1

# Leveraging smart contracts for enhanced traceability and security in bank transactions on a blockchain platform

Obamehinti Adeolu Seun*, Adekunle Eludire, Araoluwa Simileolu Filani

***Abstract.*** *Traceability of transaction have been an issue facing the financial institution for a long time. The banks are the actors who have overall responsibility for financial transaction, thus placing them in a position of responsibility for realizing the traceability demands. The bank has the coordinating role in financial transfers as well as performing tasks during transaction. Due to lack of traceability, a lot of fraudulent activities go on without being detected one of which is the issue of fake alert system, where money could assume to be transferred to a recipient account and yet not reflect in the account balance. It needs to be established that financial traceability is a problem that requires solution. In other to address these, blockchain technology which is a noble disruptive technology that is tamperproof, secure and transparent and store hash value of data is the most viable way of addressing the challenge of traceability of financial transactions.*

***Keywords***: *traceability, smart contract, blockchain, proof of work.*

## 1. Introduction

Financial traceability is the process by which a transaction is properly traced to its destination, that is, the recipient of the transaction and where the transaction emanated from. Traceability has experienced an increased importance for bank practices in recent years [1].states that bank sector sees it as a high priority on the management agenda today. Financial Traceability is often understood from environmental aspects, but it also includes the social and economic aspects of the corporation [2]. Traceability is becoming a customer requirement, pressuring corporations to further consider it. It has, however, a positive effect on the profit as well since it often becomes more efficient in its use of resources [4]. Thus, practicing Corporate Social Responsibility (CSR) can make companies improve the traceability of transactions in within the sector. The financial sector is experiencing an increasing traceability awareness within their projects. This includes both materials that have less impact on the environment which are fairly produced, as well as financial conditions and other social aspects during actual transaction [3]. The main financial institutions or banks are the actors who have overall responsibility for financial transactions, thus placing them in a position of responsibility for realizing the traceability demands. The bank has the coordinating role in financial transfers as well performing tasks during transactions. Financial traceability has it challenges over the years due to lack of a secured network system to properly manage the transparency of transaction that goes in and out of an account [7]. First, unlike blockchain technologies, bank transactions are not only centralized, but they are also backed up using third-party institutions (Bracci, 2021). Second, cryptocurrency payments are new technologies that will potentially disrupt the traditional way of bank operations especially in its level of transaction security and traceability [8]. Third, since their inception, most banks in Nigeria have their information dispersed in a wat that transaction histories are often lost [5]. Fourth, banks owners associate blockchain technology with complexity and cost concerns[6].Embracing blockchain technology is one of the most viable ways of helping financial institutions reach such milestones especially by ensuring the traceability of their assets and operations. Blockchain technology, is an innovative technology renowned for high traceability, transparency, confidentiality, irreversibility, accuracy, and delivery [10]. When it comes to traceability, blockchain technology, leverage the use of smart contracts which is an executable code that serves as policy guide in the blockchain network will ensure that every user can track the history of trusteeship and journey of an asset in real-time. As defined by the United Nations Global Compact, "Traceability is the ability to identify and trace the history, distribution, location and application of products, parts and materials, to ensure the reliability of sustainability claims, in the areas of human rights, labour (including health and safety), the environment and anti-corruption [3]. Even with favourable opportunity for fin4ancial institutions to adopt blockchain technology [11] found that existing research is yet to show the extent to which blockchain technology has the potential to promote traceability of bank activities in Nigeria. Since bank transactions over the year have had issues of accurate traceability of their activities, [12] calls for the implementation of traceability systems that can provide transparency in their operations by arguing that it is both a social and economic challenge.

Traceability has been acknowledged as an effective tool for achieving sustainability objectives in a number of businesses. This is caused by the constantly increasing demand from consumers for responsibly sourced and produced products together with the obligations by regulatory framework to improve transparency and tracking in supply chain [13]. Although other sectors, industries, countries, and regions have already started implementing traceability, bank sector are yet to tap into it despite their massive numbers and assimilation in the global economy. The traceability system of blockchain technology also facilitates the detection of fraud and secures the integrity of the supply chain globally [4]. In the context of blockchain technology, this study seeks to understand the traceability of bank transactions in other to prevent the menace of fake alert. Using Nigeria as a case study based on existing information technology-based systems and leverage on blockchain technology to provide a traceable transaction system in the bank sector. This research looks into what various sectors used different technologies for traceability, and its limitations and the need to adopt blockchain technology for traceability of transactions. Blockchain smart contract will serve as the driving force in the area of policy guidance in the transaction network. Smart contract is an executable code which helps to secure every transaction, that is carried out in the blockchain network system. The agricultural sector has already proposed a number of blockchain-based solutions to livestock data management [13] along with food traceability and safety [14]. However, this research mainly delves into how banks can implement blockchain technology-based traceability in their business context by identifying and exploring key factors that are crucial to the effective application of the systems in the traceability of transactions

## 2. Literature review

The review of literature discusses the existing practices with which banks uses to trace transaction. It also discusses a brief description of blockchain technology, layers of blockchain technology, existing systems and sectors where blockchain technology have been applied and used to solve various challenges in bank and related sectors. According to [14] blockchain technology presents unique opportunities as regards its traceability capabilities it explored the critical success factors for adopting blockchain technology to promote traceability in the supply chain of Small and Medium Enterprises (SMEs). [12] identified that blockchain technology can be used in the real estate sector, for the purpose of tenant and landlord rent. It discusses how smart contract is written as executable rule for the purpose of the real estate sector so as to provide solution to the rental challenges and a secured platform for the said transaction. Blockchain was introduced to give override to primitive business process, where trusted parties are needed for transaction verification and it also run a centralized architecture. With blockchain technology, sectors can now run a decentralized system of transaction and no need for third part interference, with credible transactions. The unique characteristics of blockchain technology has provided security, tamper proof, transparent, database for proper public record keeping according to [11]. Blockchain is regarded as a public ledger of database for public repository. According to [13] stated that blockchain can be used in banking sectors, where banks use same blockchain for customers transaction thereby providing transparency off transaction. Blockchain is also seen to be used for auditing of transactions there it was proposed by [12] for company to put resources together and invest in blockchain technology to used it to build a decentralized architecture thereby minimizing transaction cost as the technology also proffer safe, fast and transparent system

Furthermore, [10] identified that blockchain is considered beyond crypto currency, with smart contract playing a pivotal role. Also, according to [11] indicated that smart contract was considered the next level of blockchain used as executable code for transaction policy. It can therefore be said that smart contracts within the context of blockchain as embedded code run in a decentralized way used in the blockchain without the need of a centralized authority to operate the blockchain, according to [8]. Blockchain system [4] states the importance of smart contract in order to accommodate complex transaction and interaction within the limitless application. This in a way has indicated another relevance of blockchain technology. In addition, according to the research findings of [7] 33% of C-suite executives has shown interest in considering rather actively engages in blockchain.

Furthermore [11] pointed out that developers are beginning to see the effectiveness and capabilities of blockchain technology and need to explore various application depending on sectors to adopt the technology. Also, according [9] based on the audience there are three distinguished generations of blockchain which are: blockchain 1.0 this is the cryptocurrency digital transaction while Blockchain 2.0 includes smart contract, which provides a system beyond cryptocurrency and blockchain 3.0 involves science, internet of things, government and health sector. [7] states that blockchain has not covered its full capabilities. Another research was carried out by [4] on how blockchain and decentralized system can be used for internet of things and how it can also manage big data in a decentralized way this is according to [15] found that blockchain technology can be used in the real estate sector, for the purpose of tenant and landlord rent. It was clearly discussed in the research how smart contract is written as executable rule for the purpose of the real estate sector so as to provide solution to the rental challenges and a secured platform for the said transaction. According to [9] Blockchain technology can not only process currency transactions but can also ensure that transactions comply with programmable rules in the form of “smart contracts”. All these transactions could be validated between parties who fully trust each other without relying on a trusted middleman”. Honduras government has set up all land records on the Blockchain. Whenever there is a change of ownership of a property, it gets recorded openly [9]. The tamper proof and straightforward of the Blockchain technology make it fit for records, create transaction and keep record of such transactions. Presently, the majority of the establishments, such as firms, have received Blockchain innovations to keep up discreet and secure databases. Blockchain can be utilized as a legal official administration to make it simple and modest by connecting some required information with the record of transaction. [14] noted that" There are different type of consensus mechanism, the most outstanding is the Proof-of-Work (PoW). it requires solving the problem of a computational procedure, like discovering hashes with explicit examples, for example a main number of zeroes [4] found to guarantee verification and undeniable nature". In the case of power of stake, it is not determined by their mining power, Proof-of-Stake (PoS) conventions split stake block according to the present abundance of miners [13] Thus, the determination is more pleasant and keeps the wealthiest member from overwhelming the system. Numerous blockchain, for example, [5] found that ethereum are bit by bit moving to Proof of Stake (PoS) which usually requires miners to use high computational power and because of the noteworthy reduction in power utilization and improved adaptability [1]. An extra layer, the compute interface, permits blockchain to offer greater usefulness. For all intents and purposes, a blockchain stores a state which comprises for example of the considerable number of exchanges that have been made by the clients, in this way permitting the count of every client's equalization. Notwithstanding, for further developed applications we have to store complex states which are refreshed powerfully utilizing disseminated figuring, for example states that move starting with one then onto the next once explicit criteria are met. A unified blockchain is a cross breed mix of public and private Blockchain [11]. In spite of the fact that it has comparable versatility and security assurance level with private blockchain, their difference is that it has a set of hubs, named pioneer hubs, is chosen rather than a solitary element to check the transaction record. This empowers a mostly decentralized plan where pioneer hubs can allow authorizations to different clients. [12] found that on the grounds that, notwithstanding established highlights, for example, the proprietorship and the executives of the data shared in the blockchain, we consider highlights, for example, transaction endorsement time, or security perspectives, for example, obscurity. The blockchain innovation is highly secured and autonomous and also keep record of the unique finger prints of a computerized resource without putting away the advanced resource [4] "highlights all banks are currently engaged in developing a vision of what this technology means for their business". [2] discussed that in research and practice that the main parameters for Blockchain implementations such as security, data privacy. [12] discusses proof-of-work approaches that require high levels of energy but guarantee relatively high levels of consistency and protection against forgery by any actor in the network for example, in bitcoin, compete against less costly ones. Such alternative approaches require a portion of a trust in some elements of the network, such as actors based on the resources they put at risk during validation for example, the proof-of stake or in the manufacturers of devices that are used to validate transactions for example, proof-of-elapsed time in hyper-ledger saw-tooth lake. For the design and deployment of blockchain implementations [14] found that there are different selection criteria or parameters that are required to be considered while designing and deploying the implemented blockchain

## 3. Research methodology

This chapter discusses the methodology used. It explains the method approach and algorithm framework to be adopted in this research. The method and algorithms are explained in the subtopics. Steps Approach to the methodology adopted as it is shown in the figure 1.1 is stated below;

i. **The registration phase:** The registration phase allows intending participant to register with their identity, after the registration the user can login with its private key where the intending users gives is details such as name, national identification number and bank verification number. The miners, mine block using the proof-of-concept algorithm.

ii. **The Proof of work concept:** Under the proof of work data administration is taken into the ledger of the blockchain system, where the block miners are required to mine a block for the user. Upon mining this block, a user is expected to generate a private key which is for validation by the owner of the transaction. Another key which is generated is the public key which is available to every participant in the blockchain in order to verify the transaction actually belongs to the owner. Once this is done a smart contract policy is written to serve as policy guide in the blockchain system.

iii. **Smart contract policy:** The smart contract will serve as the policy guide in the blockchain system. This uses its policy which is written in solidity language to set rules in the blockchain network. After the smart contract is written then the chaotic map/ elliptic curve is used for encryption and decryption.

iv. **Transaction hash value:** This is where the transactions are saved. Every transaction in the blockchain is saved in the hash pull of data and can be recalled or generated when needed. It further provides durability of transactions. Meta-mask. This is a test-net platform where the application will be evaluated.

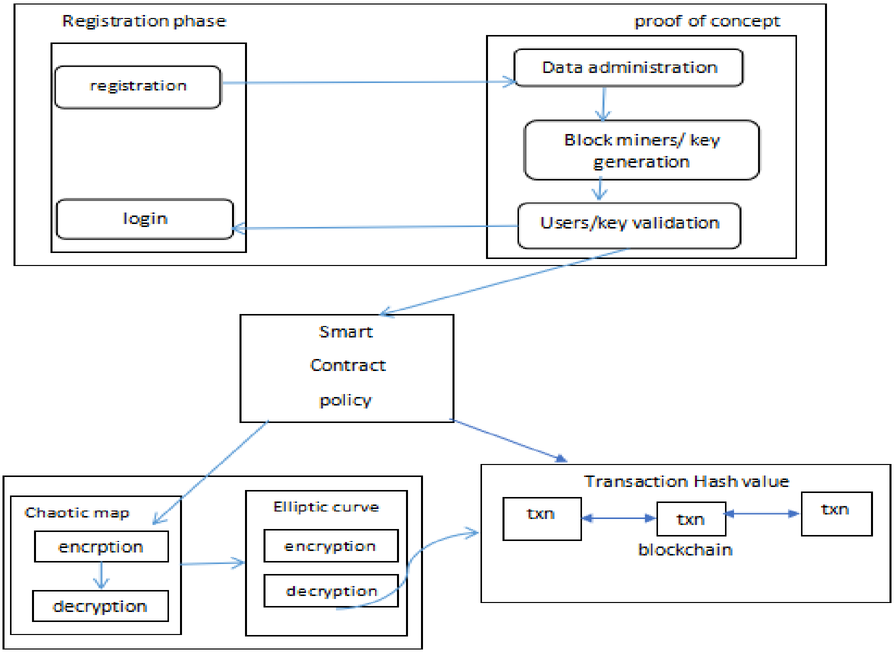

**Figure 1.** Architecture of the proposed system adopted from [9]

### *3.1. Proof of Work Concept*

The first step to achieve the desired research is to use the proof of work concept of algorithm which requires all miners on the network to solve a cryptographic puzzle by applying the brute force formula. Take for example if the ethereum blockchain has a new transaction which are tentatively committed and they are based on Proof of Work (PoW) output, a selected block created by the winning node is broadcasted to all the nodes, at specific synchronization interval. Once the block is transmitted using a peer-to-peer network to other nodes the same is included in the blockchain and any other tentative transaction are rolled back (According to (Zhao, 2018) by rule of probability the consensus is achieved by 51% if power of work in the algorithm rather than 51% people count). The proof of work concept is used in this study because compared to other algorithm it is considered secure as it is almost impossible for the concept to be attacked unless a miner acquires 51% of computing power which is made impossible by the blockchain structure. This is indicated in figure 1 architecture frame work of the proposed system.

Proof of work concept steps;
Proof of work with sha 256^2
Ethereum uses {0, 1}2^64 {0, 1} ^256▼
X sha 256 (sha 256(x)) e {0, 1} ^256▼
Given a 'target' T.E {0, 256}
To 'mine' block – data until hash<t
Nonce=next nonce
Hash= h (block – data/nonce)

There is no better way than guessing probability of success for on nonce t/2^256 T is adjusted every 2016 blocks to keep producing block every 10 minutes.

### *3.2. Smart Contract*

The smart contract is the executable code which verifies the value of the transaction and checks if it meets all the rules embedded in the contract before it can proceed to send a message through individual addresses to others. The principal parts of the smart contract are a lot of executable capacities and state factors. Every exchange has input parameters which are required a capacity in the agreement. Amid the execution of a capacity, the status of the state factors is changed relying upon the rationale usage. The smart contract code is written in abnormal state dialects, for example, Solidity and Python for Ethereum applications. The code is aggregated into bytecode utilizing compilers as Solidity or Serpent.

The agreement code will be transferred into the blockchain once the compiler is executed with no mistakes. Each agreement will be allotted a one-of-a-kind location by the blockchain system. Ethereum is one of the favored advances for the improvement of the keen contracts. The fundamental segments for the exchanges depend on state machine and capacities. The state machine is a turing-complete contract handling and execution stage based on a Blockchain decentralized shared record. The plan and the usage of the ethereum are absolutely autonomously from the digital money bitcoin. An abnormal state programming language called Solidity is utilized to compose brilliant contracts and Decentralized Applications (DApp). The software engineer can make their exchanges groups, state changes and occasions capacities, and guidelines for proprietorship. The product code is executed on a virtual machine alluded to as the Ethereum Virtual Machine (EVM).

### *3.3. Hash value veneration using Blockchain technology*

Blockchain technology verifies the user's authentication process and the hash value function generated using the transaction between the user and the banking server. The transactions performed by the user are stored in the hyper-ledger technology which is a distributed enterprise grade that provides a high level of security.

Transactions define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

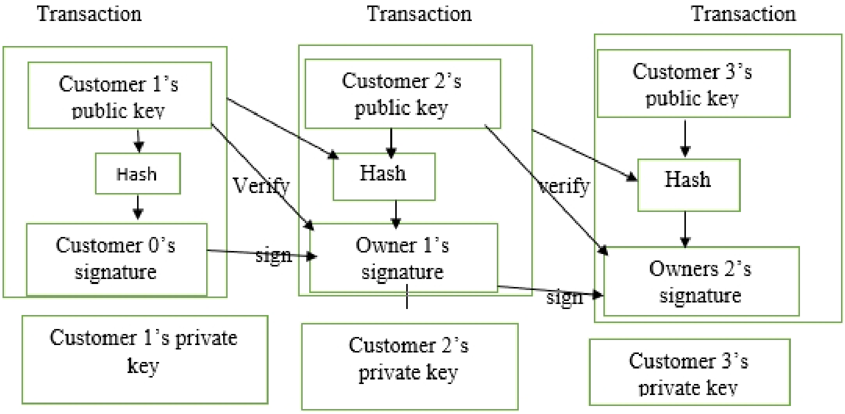

**Figure 2.** Transaction Hash Algorithm [6]

The chain of blocks is composed of multiple transactions which are composed of transaction id, previous transaction id, user's public key, the owners 0's, 1's, 2's 3's are various owners of transaction that is being stored in the hash value. The owner's signature is a private key that is used by every transaction owner in the blockchain to verify transactions before it can go through. All pf these transactions are saved in the hash which serve as data repository in the blockchain system. Low entropy password, chain code function, functional parameters, as depicted in Figure 2.

The Figure 3 depicts the components involved in the generation of 0 hash function for the Series of blocks created in the blockchain technology. The blockchain is composed of series of blocks and each block is bounded with hash value, transactions performed between the user (Ui) and the Banking Server (BSi), iterations, time stamp and the hash value of the previous block. Once the transaction is inputed, the message is interfaced with the message length counter and padding unit which in turns check the validity of the message and sends it to the message register. The sha 256 operation relate the message to the round register and hash register which finally sends it to the hashed output.

i) The chain of blocks has been created based on the hash value generated by incorporating Secure Hash Algorithm (SHA-256) as Depicted in Figure 3.

ii) The incoming message digest from the user UID is performed with Secure Hash Function (SHA-256). The new hash function is generated whenever-the comparison of existing hash value is not matched but with matching credentials.

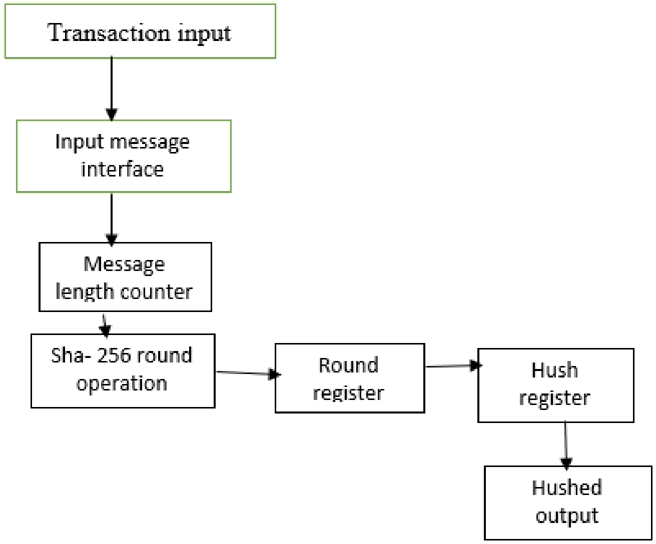

**Figure 3.** Hash Algorithm [4]

## 4. Conclusion

Traceability of bank transaction is an important factor that gives customers the desired satisfaction of the willingness to continue using a particular bank. With the aid of blockchain technology, every transaction that will be cared out within the banking system will be properly traced in other to prevent fake alert transfer.

All authors have read and agreed to the published version of the manuscript.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. M.W. Agungi, *The business blockchain promise traceability: practice, and application of the next Internet Technology*, John Wiley & Sons, Inc., 128 (2), 2022, pp. 1-16.
2. S.A. Anderson, The traceability of fees payment through banks by student to various institutions, *International Journal of Information Science*, 275 (1), 2017, pp. 1-12.
3. M. Atzori, *Blockchain bad architectures for the internet of things*, Springer, 2016.
4. O.S. Azubuike, Banking sector a critical sector addressing the bottle necks. *International of Advanced Trends in Computer Science and Engineering*, 4(9), 2019.
5. M.E. Bracci, Smart contracts: terminology, technical limitations and real-world complexity, *Law, International Journal of Innovation and Technology*, 269(3), 2021, pp. 1-14.
6. V. Buterin, Public and private blockchain, *Ethereum blog*. 45(2), 2015.
7. J.S. Chen, PayPal transactions effectives towards payment to various sectors, *International Journal of Information and Computing*, 189(3), 2020.
8. Das Mankatail, Blockchain use cases for food traceability and control, *Journal of Natural Science*, 45(2), 2018, pp. 1-13. https://www.sklkommentus.se/globalassets/kommentus/bilder/publication
9. E. Das, Privacy and security challenges in internet of things. *Journal of Distributed Computing Internet Technology,* 78(2), 2018.
10. European (2020). Effect of customer feedback on traceability.
11. P. Glaser, Towards a more democratic mining in bitcoin, 2019.
12. M. Gupta, *Blockchain for Dummies*, IBM Limited Edition. [E-book]. 2017 Available online: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=XIM12354USEN
13. S.M. Jason, *The blockchain and kudos: distributed system for educational record, reputation and reward*, Proceedings of 11th European Conference on Technology 4(2), 2019, pp. 1-12.
14. K.D. Jude, PayPal transactions effectives towards payment to various sectors, *International Journal of Information Science and Computing*, 2(21) 2020, pp. 1-13.
15. I.P. Karamitsos, Design of the blockchain smart contract; A use case for real estate. *International Journal of Management Information Technology and Engineering*, 8(4), 2018, pp. 1-6.

*Addresses:*

- Obamehinti Adeolu Seun, Joseph Ayo Babalola University, Nigeria,
  lebiobamehinti@gmail.com
  (**corresponding author*)
- Adekunle Eludire, Joseph Ayo Babalola University, Nigeria,
  aaeludire@jabu.edu.ng
- Araoluwa Simileolu Filani, Joseph Ayo Babalola University, Nigeria,
  asfilani@jabu.edu.ng